REFERENCES

Adeyinka O ,(2008), "Internet Attack Methods and Internet. Security Technology," *Modeling & Simulation. AICMS 08.*

Al-Salqan Y.Y,(2000), *Summary Report on Enterprise Security Workshop. WETICE 2000:* 139-140.

Anderson J.P,(2010), "Computer Security Threat Monitoring and Surveillance", http://csrc.nist.gov/publications/history/ande80.pdf,.

Anderson R.J, (2008) ,"Security Engineering. A Guide to Building Dependable Distributed Systems" (2. ed.), Wiley.

Bace R and Mell P,(2001)," Intrusion Detection Systems, Computer Security Division", Information Technology Laboratory, Nat'l Inst. of Standards and Technology.

Beaulieu Alan, (2009) "Learning SQL, Second Edition" Copyright *2009* O'Reilly Media, Inc., 978-0-596-52083-0."

Clifford Stoll, (2009)," Why Web Won't Be Nirvana" - Newsweek and The Daily Beast.

Dietterich T.G, (2002), "Machine Learning for Sequential Data: A Review," *Proc. Joint IAPR Int'l Workshop Structural, Syntactic, and Statistical Pattern Recognition (SSPR/SPR '02)*, LNCS 2396, pp. 15-30,.

Dokas P., Ertoz L., Lazarevic A., Srivastava J., and Tan P.N.,(2002), "Data Mining for Network Intrusion Detection,"*Proc. NSF Workshop Next Generation Data Mining (NGDM '02)*, pp. 21-30.

Gupta K.K, Nath B, and Kotagiri R.,(2006) ,"Network Security Framework," *Int'l J. Computer Science and Network Security*, vol. 6, no. 7B, pp. 151-157.

Gupta K.K, Nath B, Kotagiri R., and Kazi A, (2006), "Attacking Confidentiality: An Agent Based Approach," *Proc. IEEE Int'l Conf. Intelligence and Security Informatics (ISI '06)*, vol. 3975, pp. 285-296.

Gupta K.K, Nath B., and Kotagiri R, (2007), "Conditional Random Fields for Intrusion Detection," *Proc. 21st Int'l Conf. Advanced Information Networking and Applications Workshops (AINAW '07)*, pp. 203-208,.

Ji C and Ma S.,(1997) "Combinations of Weak Classifiers," *IEEE Trans. Neural Networks*, vol. 8, no. 1, pp. 32-42.

Kartalopoulos S.V,(2008)," Differentiating Data Security and Network Security." ICC 2008: 1469-1473.

Kim D.S and Park J.S, (2003) “Network-Based Intrusion Detection with Support Vector Machines,” *Proc. Information Networking, Networking Technologies for Enhanced Internet Services Int’l Conf. (ICOIN ’03),* pp. 747-756.

Klein D and Manning C.D,(2002) “Conditional Structure versus Conditional Estimation in NLP Models,” *Proc. ACL Conf. Empirical Methods in Natural Language Processing (EMNLP ’02),* vol. 10, pp. 9-16, Assoc. for Computational Linguistics.

Kruegel C., Mutz D., Robertson W., and Valeur F.,(2003) “Bayesian Event Classification for Intrusion Detection,” *Proc. 19th Ann. Computer Security Applications Conf.* (ACSAC ’03), pp. 14-23.

Marin G.A and Song Luo,(2005) “Realistic internet traffic simulation through mixture modeling and a case study “*WSC '05: Proceedings of the 37th conference on Winter simulation* .
.

McHenry J. T and Dowd P. W , (1998) ,”Network Security: Its Time to Take It Seriously”, *IEEE Computer*, pp. 24-28.

Philip Boyle and Kevin D. Haggerty,(2009),” Spectacular Security: Mega-Events and the Security Complex”, *International Political Sociology 3*, 257–274.

Portnoy L., Eskin E, and Stolfo S, (2001), “Intrusion Detection with Unlabeled Data Using Clustering,” Proc. ACM Workshop Data Mining Applied to Security (DMSA).

Shah H., Undercoffer J, and Joshi A, (2003) “Fuzzy Clustering for Intrusion Detection,” *Proc. 12th IEEE Int’l Conf. Fuzzy Systems (FUZZ-IEEE ’03),* vol. 2, pp. 1274-1278.

Steve Friedl's, (2010),”Unixwiz.net Tech Tips An Illustrated Guide to IPsec” .

Wang W, Guan X.H, and Zhang X.L,(2004), “Modeling Program Behaviors by Hidden Markov Models for Intrusion Detection,” *Proc. Int’l Conf. Machine Learning and Cybernetics (ICMLC ’04),* vol. 5, pp. 2830-2835.

Warrender C., Forrest S., and Pearlmutter B., (1999) “Detecting Intrusions Using System Calls: Alternative Data Models,” *Proc. IEEE Symp. Security and Privacy (SP ’99),* pp. 133-145.

Witten I.H and Frank E, (2005), “Data Mining: Practical Machine Learning Tools and Techniques”, Morgan Kaufmann.

Yu Gu, Andrew McCallum, Don Towsley,(2005)”Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation”,Department of Computer Science,University of Massachusetts.

Yuval Fledel, Robert Moskovitch, Yuval Elovici:Asaf Shabtai, Dennis Potashnik, (2011)," Monitoring, analysis, and filtering system for purifying network traffic of known and unknown malicious content". Security and Communication Networks 4(8): 947-965.

Zhang Z, Li J., Manikopoulos C.N., Jorgenson J., and Ucles J., ( )"HIDE: A Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification," Proc. IEEE Work